## CLAIMS

What is claimed is:

1. A method of detecting a malware comprising the steps of:

monitoring file access operations of a process;

intercepting a file access operation of the process to a file;

waiting a time interval; and

scanning the file for a malware.

2. The method of claim 1, wherein the process is associated with an application program.

3. The method of claim 1, wherein the file access operation is a file write operation.

4. The method of claim 1, wherein the file has a specified file type.

5. The method of claim 1, wherein the time interval is predefined.

6. The method of claim 1, wherein the time interval is user-defined.

7. The method of claim 1, wherein the time interval is based on a filetype of the file.

8. The method of claim 1, wherein the time interval is based on the process.

9. The method of claim 1, wherein the malware is a computer virus.

10. The method of claim 1, wherein the malware is a computer worm.

11. The method of claim 1, wherein the malware is a Trojan horse program.

12. The method of claim 1, further comprising the step of:

allowing the intercepted file access operation of the process to a file to complete.

13. The method of claim 12, further comprising the step of:

allowing at least one additional file access operation of the process to a file that occurs before the scanning of the file for a malware to complete.

14. A system for detecting a malware comprising:

a processor operable to execute computer program instructions;

a memory operable to store computer program instructions executable by the processor; and

computer program instructions stored in the memory and executable to perform the steps of:

monitoring file access operations of a process;

intercepting a file access operation of the process to a file;

waiting a time interval; and

scanning the file for a malware.

15. The system of claim 14, wherein the process is associated with an application program.

16. The system of claim 14, wherein the file access operation is a file write operation.

17. The system of claim 14, wherein the file has a specified file type.

18. The system of claim 14, wherein the time interval is predefined.

19. The system of claim 14, wherein the time interval is user-defined.

20. The system of claim 14, wherein the time interval is based on a filetype of the file.

21. The system of claim 14, wherein the time interval is based on the process.

22. The system of claim 14, wherein the malware is a computer virus.

23. The system of claim 14, wherein the malware is a computer worm.

24. The system of claim 14, wherein the malware is a Trojan horse program.

25. The system of claim 14, further comprising the step of:

allowing the intercepted file access operation of the process to a file to complete.

26. The method of claim 25, further comprising the step of:

allowing at least one additional file access operation of the process to a file that occurs before the scanning of the file for a malware to complete.

27. A computer program product for detecting a malware comprising:

a computer readable medium;

computer program instructions, recorded on the computer readable medium, executable by a processor, for performing the steps of

monitoring file access operations of a process;

intercepting a file access operation of the process to a file;

waiting a time interval; and

scanning the file for a malware.

28. The computer program product of claim 27, wherein the process is associated with an application program.

29. The computer program product of claim 27, wherein the file access operation is a file write operation.

30. The computer program product of claim 27, wherein the file has a specified file type.

31. The computer program product of claim 27, wherein the time interval is predefined.

32. The computer program product of claim 27, wherein the time interval is user-defined.

33. The computer program product of claim 27, wherein the time interval is based on a filetype of the file.

34. The computer program product of claim 27, wherein the time interval is based on the process.

35. The computer program product of claim 27, wherein the malware is a computer virus.

36. The computer program product of claim 27, wherein the malware is a computer worm.

37. The computer program product of claim 27, wherein the malware is a Trojan horse program.

38. The computer program product of claim 27, further comprising the step of:

allowing the intercepted file access operation of the process to a file to complete.

39. The computer program product of claim 38, further comprising the step of:

allowing at least one additional file access operation of the process to a file that occurs before the scanning of the file for a malware to complete.